

Rules of Behavior for All Systems

The following rules of behavior apply to every VA employee, including contractors, volunteers and business partners, who have access to VHA automated information system (AIS) resource(s). Because written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using their best judgment and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, VA and VHA Directives. As such, there are consequences for non-compliance with the rules of behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension from work, demotion, removal, and criminal and civil penalties.

FOR PRIVILEGED USER (i.e., system managers, programmers, ADPAC, technical support, help desk etc.): I understand that as a privileged user I must perform my duties with special care to avoid compromising information security.

WORK AT HOME: I understand that the same security measures apply no matter where I am located. I will protect information in a manner consistent with its value, sensitivity and criticality. I will protect VA equipment by ensuring the latest anti-virus software is installed. I am prohibited from altering the configuration on government equipment unless authorized. I am required to make adequate backups of work related files housed on my home computer. I will physically protect VA equipment from abuse, use by Non-government employees, and alterations of approved software and hardware configurations. I will be responsible for the protection of all data located on VA equipment.

USE OF INTERNET: I will comply with local policies and procedures regarding my use of the Internet. I will corroborate information found on the Internet prior to its use for business decision-making purposes by consulting other sources. I will screen all non-text files downloaded from non-VA sources via the Internet with virus protection software prior to being used. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system. I understand that using VA resources to access the Internet are subject to monitoring.

E-MAIL/FAX/FILES: I understand that as a VA employee, I must not compromise or breach the organization's security by transmitting, storing or receiving communications that are discriminatory, harassing, obscene or inappropriate, abusive, profane or otherwise illegal. I understand that electronic mail is not inherently confidential and I have no expectation of privacy in using it. I understand that I am responsible for the content of all communications that are stored or sent using my e-mail account.

I understand that, when using the above resources(s), I am personally accountable for my actions and that I must:

- a. Protect sensitive information (including electronic protected health information (ephi)) from disclosure to unauthorized individuals or groups;
- b. Acquire and use sensitive information only in accordance with the performance of my official government duties, utilizing established security policies and procedures. This includes: properly disposing of sensitive information contained in hardcopy or softcopy, as appropriate, and ensuring that sensitive information is accurate and relevant for the purpose for which it is collected, provided and used;
- c. Protect information security through effective use of my access codes and devices;
- d. Protect my access codes, passwords and devices from disclosure;
- e. Protect my computer equipment from damage, abuse and unauthorized use;
- f. Report security incidents and vulnerabilities to the ISO;
- g. Comply with all copyright licenses associated with the resource;
- h. Comply with the personal use of government equipment in accordance with my site's local policies and procedures;

I understand that management has the right, in the course of an official investigation to monitor, intercept, read, record and copy all information attributable to my access of this resource.

I understand that all conditions and obligations imposed upon me by these rules apply during the time I am granted access to these systems.

I acknowledge receipt of and understand my responsibilities, and will comply with the rules of behavior for the resources defined above.

Signature, Title

Date

Printed Name

Dept. Ext.

Department Supervisor Signature

Date